Discovering University Worlds

Research Group

Working Paper #1

June 23, 2020

David Allens, Leslie Chan, Nikita Chirila, Mariana Valverde

Preliminary Findings

When public universities contract with 'ed tech' vendors: issues concerning 'Learning Management Systems' and online learning

What is a university? In Canada, as elsewhere, it is a centre for research and teaching, supported in part by public funds. It is also an employer, a producer of images, a subject of rankings, a real estate owner, a generator of revenues, and a hub in global networks of value and aspiration. But how does a university work? What exactly does it do? What are the powers and pressures, the practices and networks that constitute contemporary university worlds?

An interdisciplinary team of faculty at the University of Toronto, we seek to discover the many worlds of our own institution, in collaboration with graduate and undergraduate students. We foreground the everyday experience of people who work or study in different corners of the institution, who live in its shadow, or respond to its public face.

A pilot phase 2019-2021 has been funded by the Social Science and Humanities Research Council of Canada (SSHRC) Insight Discovery Grant #430-2019-00054

For more information about the project please contact universityworlds@outlook.com

Visit our website at http://universityworlds.ca/

To cite this paper:

Allens, D., Chan, L., Chirila, N., & Valverde, M. (2020) *When public universities contract with 'ed tech' vendors: issues concerning 'Learning Management Systems' and online learning*. Working Paper 1, Discovering University Worlds, University of Toronto.

Contents

Abstract

This paper presents early findings of research on two timely topics. The first concerns problems plaguing the U of T's chosen provider of learning software, Canvas: extensive data mining with no possibly of withholding consent; lack of transparency about the actual or potential monetization of that data and resulting algorithms; and the surveillance risks to U of T faculty and students posed by the fact that Canvas stores all of our data on Amazon Web servers. These problems are common in for-profit 'ed tech' systems, not just Canvas, but there are some non-profit community-governed alternatives which we will explore in due course. The second topic concerns international students' vulnerability to surveillance and state control when taking U of T courses online, if they are physically in home countries that exercise digital surveillance and/or censorship. Little is known about the extent to which state digital surveillance by various state security bodies is or will be extended to online courses offered by foreign universities, beyond the well-documented situation of Internet censorship in China; but we want to alert colleagues and begin to collect relevant information. We hope that students and faculty both in our own university and in others will share with us any information they have that is relevant to these concerns, by contacting Prof. Leslie Chan or Prof. Mariana Valverde at lesliekw.chan@utoronto.ca or m.valverde@utoronto.ca, respectively.

Scope of this report

As part of a larger research project on aspects of the university's internal governance, a small group is researching the university's procurement practices regarding educational software. Faculty and students are to a large extent obligated to use, and to generate data for, certain systems that the university has acquired from for-profit US based corporations whose data practices, including data mining, are nontransparent and problematic. The rapid shift to 'online learning' makes it even more imperative to collect and share information about the effects and consequences of features of various systems and products that together function as an infrastructure we must all use.

The U of T has a very significant contract with Microsoft (the reason why we are more or less compelled to use Microsoft Word, Outlook email, etc.), which we will attempt to obtain and analyze for purposes of a future fuller report; but the present preliminary report focuses on the Canvas system (known as Quercus at U of T), since it is the one through which much teaching/learning, especially online communications, happens, and the one where data mining poses a clear and present danger to faculty and students and to the public missions of the university.

As the summer unfolds we will try to delve into the procurement process, to find out whether university representatives properly uphold the digital rights and interests of faculty and students in negotiations for software licences, but that will take time and effort.

This preliminary report has two parts. The first concerns the Canvas system, the software that the U of T, along with many other institutions, chose to replace the previous system, BlackBoard, in 2017. It puts Canvas in the context of 'Learning Management Systems' and 'Online Program Managers', increasingly popular products of the sector calling itself 'ed tech'. In keeping with the stated aims of the 'Discover University Worlds' research project, we explore the effects of the corporate structure that underpins the Canvas system, which has changed significantly since the university initially chose it. This first part is mainly authored by David Allens, an undergraduate in Criminology/Socio-legal Studies, working under the supervision of Profs. Leslie Chan and Mariana Valverde. The second, briefer part reflects on the risks to many students, especially internationally students taking online courses from outside of Canada, that are posed by the

surveillance and censorship mechanisms in various states, China in particular but other countries as well. These risks will increase greatly if the students are physically in their countries of origin and thus especially vulnerable to state digital and in-person security practices.

Most of the risks to the privacy and human rights of the U of T students physically located outside of Canada that we outline here are not specific to Canvas, or to any particular university. Nikita Chirila, MA student in Criminology-Sociolegal Studies, contributed significantly to this second part, as did several colleagues from U of T and elsewhere; he will continue this research part-time over the summer under the supervision of Prof. Mariana Valverde. We urge colleagues both at U of T and elsewhere who have relevant information to contact us (though either Prof. Leslie Chan or Prof. Mariana Valverde).

Part 1: Outsourcing 'Learning Management Systems' to the for-profit 'ed tech' sector

Many tertiary institutions in North America have concluded that outsourcing is the most efficient way to implement a robust 'learning management system' (LMS, in tech industry lingo). The shift to online communications prompted by the pandemic has greatly increased the power of the companies that provide such software. A recent article by South African colleagues states that over the next five years, the EdTech corporate sector is expected to experience expedited growth (Ivancheva & Schwartz, 2020). Platforms developed by for-profit tech companies have large upfront software development, data storage and maintenance costs that institutions – such as U of T – are rarely willing to shoulder. Thus, like school boards and community colleges, public universities have for some time now turned to 'online program managers' (OPMs) that promise technically superior systems at a lower price than the university might pay if it wanted to run and control its own system and its own data. The U of T's press release announcing the contract with Canvas in 2017 voices the rationales generally used to justify this kind of outsourcing (McCahan & Hyman, 2017).

One study which examined over one hundred agreements between vendors and publicly-funded tertiary institutions, and spoke to over two hundred institutions, is a rare source shedding light on the implications for public universities and their faculty and students of outsourcing 'learning management

systems' to for-profit tech companies. (Incidentally, in the discourse of 'ed tech' the assumption is always made that the interests of the institution coincide with the interests of students and faculty, a problematic assumption, in the data world as in other areas.)

This study, published as a report for The Century Foundation, concluded that companies develop a "more aggressive and singly-focused [mindset] on maximizing return" while their public or non-profit counterparts have restrictions preventing this (Mattes, 2017). It is important that when universities (e.g U Michigan) have good data protection policies and make these public, which is in any case not common, the policies usually apply only to the university's own data collection and storage practices, not to data collected by software vendors[1]. The Century Foundation report (the only one we have located where the author read contracts between the university and the tech providers) states that these OPMs "owe no loyalty, financial or otherwise" to end users (i.e. faculty and students) and are highly likely to prioritize profit over their interests (Mattes, 2017). While this is especially true for OPMs that use a revenue-sharing pricing model to provide curricular design and other services including admissions and student career counselling whose owners usually get between 30 to 50% of the tuition paid for online course (Mattes, 2017), those systems that only provide educational technology such as Canvas also pose problems.

The OPMs that focus on providing education technology rather than the larger suite of services may not be privatizing activities such as admissions and counselling, but they use a business model that focuses on leveraging the data-sets generated as students learn and instructors teach. They are thus an integral part of the trend known as 'data extractivism'.

A recent study that focused on Canvas concluded that "institutions of higher education are currently ill-equipped to protect students and faculty required to use [Instructure's Canvas learning management system] from data harvesting or

---

[1] The University of Toronto seems to be elaborating a policy for its own data collection – see data.utoronto.ca/governance. However, it is troubling that U of T relies a great deal on Tableau, a popular data visualization software acquired by Salesforce for $15.3b US. This matters because Salesforce is the biggest 'customer relationship management' firm in the world, and may well be offering U of T services with problematic implications.

exploitation" (Marachi & Quill, 2020). Our preliminary research suggests that this is the case at U of T, though as mentioned above we plan to do more research including interviews with administrators and staff members to fill out the initial picture and provide more information.

Canvas/Quercus

Founded in 2008, Instructure, Inc. is now the developer and publisher of the Canvas LMS (Quercus is part of Canvas). The system is currently the US-based company's flagship product. While no information is readily available on the number of universities that use Canvas, the platform grew from 20 million users in 2018 to over 30 million users in July 2019 (Amigot, 2019). Canvas is now the leading LMS, having replaced Blackboard in many cases including U of T (Mckenzie, 2018).

According to Instructure's former CEO, this market share has given the company "the most comprehensive database on the educational experience in the globe" (Hill, 2019). What data is being collected is not apparent to the 'end user' (that is, instructors and students). But their privacy policy openly admits that in addition to "user-provided data" (i.e. information willingly presented to the site, such as data used to set up an account, or data that must go through the system, such as information transferred between users), Canvas also collects the following data:

- Browser type, operating system, IP addresses, domain name, time stamps
- What users searched for and viewed; web beacons and cookies to log interactions with the site; how often user visits the website; what Instructure pages they visit; and other places visited before coming on the site.
- How long students spent reading texts or otherwise engaging with each course material

All of this so-called "collected" data, which again, is over and above data generated as students and instructors provide 'content', may be connected to personally identifiable information (Instructure, 2019). The cookies in a student's laptop, for example, provide a great deal of information about the person who owns and uses the laptop.

Instructure is explicit about its business model, which offers services such as career advice (Hill, 2019). However, many universities do not include this, or

admissions, in their purchasing agreements[2]. The career advice is likely based on algorithms obtained by de-identifying and aggregating and then analyzing all of the data mentioned above, aggregating the data across institutions and jurisdictions and most probably, as is generally done in the world of big data, linking the data sets that the company generates and controls to existing public or privately owned data sets (Instructure, 2019).

The former CEO stated a year ago that the company has already gone through "enough cycles thus far to have demonstrable results around improving outcomes with students and improving student success" (Hill, 2019). The ultimate aim of the company is to use the data collected to create a **predictive model** powered by **artificial intelligence and machine learning**. To achieve this end it is necessary to possess data from a large number of institutions. Instructure is in a unique position to develop predictive models since it has "the most comprehensive database on the educational experience in the globe" with no other company having the adequate "data assets at their fingertips to be able to develop [similar] algorithms and predictive models" (Hill, 2019) –models that can draw conclusions about a student's performance in a course "even before they set foot in the classroom" (Wan, 2019). The company is third only to Google and Microsoft in the amount of student data it maintains (Menard, 2019, as cited in Marachi & Quill, 2020, p. 419).

One question for the second phase of our research will be whether the data collected by Microsoft through its contract with U of T is or could be made available to Instructure, either at the smaller scale of the institution or at the larger scale of multi-institutional aggregation. And while Microsoft and Canvas are the most visible software providers with which the university has an agreement, there are other vendors (e.g. the makers of Tableau, the data visualization software; LinkedIn, which is owned by Microsoft) whose agreements with the university and whose technical features are of interest.

It should be noted that we have no information on whether the University of Toronto or any other Canvas customer in the post-secondary world is itself in the market for the algorithms that are or will be generated out of students' and

---

[2] The scant information available suggests that vocational institutions and lower-ranked colleges sometimes pay much more for their contracts with companies such as Instructure than high-end research institutions, probably because they purchase additional services such as counselling, admissions, alumni tracking, etc.

instructors' online activity; but we will be pursuing the issue of the actual or potential market for algorithms derived from the data we generate. In the post-COVID world in particular, administrators may well be willing to pay good money for an algorithm that predicts, for example, whether students who take all their courses online are more likely to drop out than other students.

Instructure is clearly aware of the potential reputational and market share risks posed by such personal-information scandals as the Cambridge Analytica/Facebook story. Thus, Instructure's CEO claimed in 2019 that the company's "first and primary tenet is that the student, **the individual and the institution own the data**" and the company is "not looking to sell data assets," (Wan, 2019). Yet, a 2018 Common Sense Media analysis gave Canvas a 36/100 for student privacy, as "it is unclear whether student data collected on the LMS will be sold to third-parties, shared for advertising purposes, or whether the data harvested will permit third-parties to create advertising profiles used in targeted advertising" (Marachi & Quill, 2020, p. 425). Our own analysis confirms that the company's claims about us 'end users' owning our data are misleading, for several reasons. (Student data collected by the university, e.g. through ROSI, such as their grades, are not owned by the student, but are subject to data protection laws and policies; however, the data generated through using Canvas are in a different category).

First, the company claims it is "not looking to sell data assets," perhaps because it does not sell raw data. The valuable product being developed are the algorithms (predictive models) that are or will be built out of the vast amounts of data gathered across institutions and jurisdictions. Secondly, the former CEO mentioned that there is no *sale* of data. In many instances, the data do not need to be *sold* to anyone, as institutions have already consented to it being shared, perhaps inadvertently due to the misleading nature of the corporation's communications. Instructure's privacy policy explicitly allows for data to be shared with its third-party vendors (for example Amazon Web Services) "for the sole purpose of providing the Services" offered through Instructure's site (Instructure, 2019). These are *Instructure's* third-party vendors. However, because Canvas, which started out as an open-source program, is compatible with a large number of add-ons, *institutions* have the option of using third-party vendors such as Zoom, Microsoft, etc. Whether data are or can be transferred from one system/app to another, and shared without an outright 'sale', is a

huge question. Data are not like physical goods. If one owns a laptop, then nobody else can claim ownership to it. But data can be notionally said to be the property of the person generating them while still being exported or copied an infinite number of times.

This is a serious concern. In the United States, "education records and personally identifiable information can be released to third-party vendors *without consent* provided that these third-parties remain under the direct control of the institution" (Marachi & Quill, 2020, p. 426). Unless there are regulations that explicitly prevent this in Canada[3], it is likely that third-party vendors work similarly across jurisdictions. In the case of U of T, depending on the provisions of these third-party agreements, these applications may have access to "user information and SIS feeds from ROSI" (University of Toronto, 2017), a point mentioned, as if it were a plus, in the official press release announcing the university's contract with Canvas.

To make things much worse, the corporate structure of the firm means that it is no longer solely up to Instructure to decide how data will be used. Instructure, its data sets from Canvas, and resulting predictive algorithms and insights were sold in early 2020 to the private equity firm Thoma Bravo, for approximately $2 Billion USD (Thoma Bravo, 2020). No doubt the value of the company is now considerably higher, given the sharp increase in online learning. Being owned by a private equity fund means that Instructure is no longer listed in the stock market and has none of the disclosure obligations that listed companies have. As a part of the sale to or take-over by the Bravo fund, the Instructure CEO stepped down from his role (Millward, 2020), with a search still underway for a replacement. There is thus great uncertainty about the company's future direction, about the stability of any previous commitments surrounding data usage or perhaps sale, and about who will ultimately make decisions that greatly affect both universities and individual members of the university

[3] The federal government is currently contemplating updating the outdated privacy and data protection laws that we have, and the office of the federal Privacy Commissioner has recently conducted consultations on the regulation of algorithms that are particularly relevant to contracts with Canvas, but as of this writing there is no draft legislation.

community. The current/interim CEO of Instructure is a Thoma Bravo operating partner.

The corporate structure behind Canvas is crucial: the affiliates clause of Instructure's privacy policy states that the company "**may share some or all of [its user data or] information with [its] Affiliates" which refers to "[a] parent company, any subsidiaries, joint ventures or other companies under a common control**" (Instructure, 2019). Including Instructure, there are 43 companies under the 'common control' of Thoma Bravo (Thoma Bravo, n.d.). Other companies are also owned by the fund, to a total of 73, but possibly without direct control. Observers have noted that Thoma Bravo has been on a **"cybersecurity acquisition spree**" with ten of its eleven cybersecurity/identity and access management companies being acquired in the last three years (Ghosh, 2019). Another ten software infrastructure firms in the portfolio deal with areas such as automation, the improvement of information-driven interactions between businesses and customers, and perhaps most notably, data analytics to identify and predict and customer behavior (Infogix) through real-time analysis (Empirix) and collation from multiple sources (Qlik) (Thoma Bravo, n.d.).

Canvas uses a take-it-or-leave-it contract style that does not appear to provide an opportunity for anyone beyond the university's designated signatory to provide consent (Instructure, 2018a). We know this from our personal experience, since we are not asked to click any 'I accept' button the first time we use the Canvas system. This means that so-called 'end-users'– faculty and students – do not have an opportunity to opt-out of data collection or be informed of the use of said data (Instructure, 2019). When asked about any end-user ability to opt out of data use for things like the company's proposed predictive model, or to have data generated by them deleted, Instructure's former CEO sidestepped the question by saying, "it does not necessarily work that way, per se" --before saying no one has made that request.

In the EU, 'end users' such as students can ask for their data to be removed from a system such as Canvas even if they were not the original 'customers' through the EU's 'right to be forgotten' law. That right is limited in the current algorithm-focused tech world, since data could well have been shared with multiple companies and used to develop multiple algorithms before the course ended and the student made the request. However, in Canada we do not have even that minimal right to ask for our data to be deleted.

Further, as was pointed out years ago by University of Toronto critics of the university's initial contract with Microsoft (Bohaker et al., 2015), because Instructure is an American company, and the data are not stored in Canada, Canvas/Quercus users are not covered under Canadian data protection laws. (The same applies to numerous apps used by millions of Canadians, incidentally; if a Canadian wants to sue Uber or Airbnb, for instance, for misfortunes that took place in Canada, they must go to or find a lawyer in the European low-tax capitals where those companies have their non-US headquarters.)

Where are our data? The myth of "public" clouds

Canvas and LMS like it are cloud-based products. That means that data generated by university members using the system are stored not in a local server but in large-scale multi-purpose servers whose location is semi-secret but is most likely to be within the US. This provides numerous benefits including resiliency through backups, data management, and protection that is beyond the average school's budget (Instructure, 2018b). However, private servers, that is, servers owned and controlled by an institution, offer increased control. Control is thought by informed observers to be the best way to speak about data governance issues today, when selling personal information to advertisers is no longer the sole or main business model in the tech sector. Some knowledgeable observers of the algorithm business observe that the right to privacy is no longer useful nor effective when dealing with companies that analyze vast amounts of de-identified data. They suggest that the quest for 'privacy by design' long touted by former Ontario privacy commissioner Ann Cauvokian should be replaced by "**control by design**" (Centre for Digital Rights' submission to the Office of the Privacy Commissioner of Canada's consultation on the regulation of artificial intelligence, March 18 2020).

What 'control by design' would mean depends on the context. In the case of the now abandoned Sidewalk Labs project for Toronto's waterfront, for example, the advocates of control by design wanted to ensure community control over data gathering in public spaces, including the initial decisions on whether collecting a particular kind of data is necessary or desirable. In the university context, local 'control' over data collection and data governance would have to be spelled out, since the institution, as mentioned above, may have interests (e.g. in software to predict student behaviour or to evaluate

faculty performance) that are separate from and perhaps in conflict with the interests of faculty and students.

Many government bodies and large businesses use private servers rather than US corporate 'clouds' in order to avoid possible security breaches, to ensure users' access to the data protection laws and the courts of their own country, and to mitigate other risks that so-called 'public' servers pose. (Note that 'public' in tech speak does not mean public. When data are 'uploaded to a public cloud' what happens is that data are sent to and stored in corporate, not public, servers that are located on a piece of land that is not under heavenly jurisdiction but within the jurisdiction of the relevant state. The phrase 'a public cloud' actually refers to a group of servers owned by a single company but housing data from many different customers.)

Canvas stores user data[4] in "geographically diverse Amazon Web Services (AWS) data centers" (Instructure, n.d.). If we assume that WikiLeaks doxxing of AWS data centers is accurate – and that there have been no changes since late 2015 when the document was written, (WikiLeaks, 2018) –there are no Amazon Web centers in Canada. (Knowledgeable people confirm this, though maps of Amazon web servers appear to be highly secret.) Despite the global power of Amazon, AWS has proven to be vulnerable to data hacking with several high profile security breaches, including one that left Tesla vulnerable to cryptocurrency mining (Marachi & Quill, 2020).

Incidentally, the competing Canadian D2L firm, used at the University of Ottawa as well as at many Canadian colleges, also stores university-generated data in the Amazon 'cloud', though whether that information about data storage, and its legal consequences, is clearly divulged to the institutions that have chosen D2L instead of Canvas is not clear.

---

[4] Our focus here is on what does or might happen to the data of 'end users', students and instructors; but whether companies such as Canvas also engage in data mining that appropriates an institution's information about itself is an interesting question worthy of further study. The legal separation of 'customers' (institutions) from 'end users' does not mean that institutions have data protection.

The loss of the protection that Canada's admittedly weak privacy and data protection laws give is not adequately communicated to end-users. Our personal experience and that of colleagues suggests that when professors and students are told they must use the system they are never told about either Instructure's data gathering practices or about the risks that the use of Amazon Web servers pose. It is not clear at this point if Instructure provides hosting options on anything other than AWS; that is, it is not clear whether any university in Canada could use Canvas but insist on having all its data stored in Canada in order to facilitate access to the laws and courts of our own jurisdictions, while also evading the eagle eye of the American agency NSA, or at least making the NSA's surveillance less easy. (It should be added that the new NAFTA, the USMCA free trade agreement, may pose some new problems for those who insist on data remaining in the national territory, though whether the 'free travel of data' provisions that will come into force July 1 apply to universities as well as governments is not at all clear.)

Current law enforcement practices are such that when data originating in Canada goes through and/or is stored in the US, the American National Security Agency (NSA) has access to all of it, not just metadata as is the case with US citizens' data. Further, we understand that over the past several years, the Communications Security Establishment (CSE) and Canadian Security Intelligence Service (CSIS) can ask for – and in the past has obtained – information on Canadian citizens that it could not itself legally collect, but which the NSA can collect and share as a "Five Eyes" ally (Levin, 2013; Ling, 2017). Students and faculty with precarious immigration status are particularly at risk.

Canadians unwittingly using a so-called cloud, largely or perhaps wholly composed of server farms on American soil, is hardly unusual. The current market for cloud-based computing is dominated by three companies – Amazon's AWS, Microsoft's Azure, and Google Cloud, with Alibaba Cloud close behind (Stalcup, 2020). A February 2020 report found that that the combined market share of these companies is at 61.4% – AWS with 32.4%, Azure with 17.6%, Google Cloud at 6%, and Alibaba Cloud at 5.4% (Canalys in Stalcup, 2020).

The selection of Instructure's Canvas was a choice made by the university after it had also negotiated with the Canadian company D2L (Desire2Learn), which produces the LMS called Brightspace. D2L is a rare Canadian vendor but unfortunately it too uses a cloud-based framework stored on AWS (D2L, 2016).

In concluding this section we draw attention to the issue of choice, institutional choice that is, and present some tentative recommendations for discussion amongst the 'discovering university worlds' research group and in the broader U of T community.

A. 'Technical' choices can have unintended effects and thus need non-technicians' ongoing input. In 2017 the Canvas system was probably a good choice, technically and financially, and there might have been no reason to suspect, at that time, large-scale data mining. But the 2020 acquisition of Instructure by a private equity firm that also owns many cybersecurity and 'identity' and data analytics firms should have sounded the alarm. We do not here criticize the university staff who made the choice of Canvas in 2017. Instead, we call for transparency, accountability, and collegiality in the procurement of software that we are all obliged to use; and, secondly, we call for a transparent process by which procurement choices are subject to review and to community discussion of the pros and cons of different alternatives.

B. Considering non-profit and community-governed software systems. Other Canadian universities use Sakai or Moodle instead of Canvas or D2L. Neither of these systems promote or encourage data mining and do not store data they collect in a US-based cloud. In our subsequent report, later in the summer, we will present more information about possible alternatives to Canvas, to spark a collective discussion that includes desirable technical features but also 'control' issues, such as individuals' ability to consent or withhold consent to data collection and the collective interest in resisting 'data extractivism' that makes profitable algorithms out of the everyday interactions that make up teaching and learning.

Part 2. International students' risks while accessing online courses from outside of Canada

Around 60% of international students in U of T's undergraduate and graduate programs come from China, where, as is well known, the Internet is highly censored. For example, if a U of T student in China is asked to watch a YouTube video, or read a New York Times article, this is not possible unless the student uses

the circuitous route to access the Internet known as a VPN (Virtual Private Network). However, while not explicitly illegal in China, the Chinese government has made it increasingly difficult to access and use VPNs by blocking most websites they may be hosted on or keeping them off mobile app stores. Two Chinese-Canadian professors with recent research and teaching experience in China told us that while government enforcement against VPNs in the past was comparatively lenient, today it is becoming evermore difficult to access websites outside of China or the VPNs necessary to do so. In addition, one of these experienced colleagues pointed out that students who use a VPN may encounter problems when accessing mainstream Chinese apps and systems because their IP address appears suspicious; as a result, most Chinese students might simply decide not to bother using VPNs while in China.

But the ability to access all compulsory or suggested course content is not the only or perhaps even the main risk faced by students studying from their home countries – not just in China, but in other states that engage in both digital and in-person surveillance and control of their residents (a category that does not exclude Canada). A problem that requires urgent collective discussion concerns the possible surveillance by various state agencies of U of T courses dealing with 'sensitive' issues, such as human rights, Indigenous movements, ethnic and religious minority rights, international conflicts, etc. We note that there are issues routinely mentioned in a large number of U of T courses that are sensitive in/for one particular country (such as the status of Taiwan and Hong Kong for China, the legitimacy of the Maduro government for Venezuela, or the legitimacy of Putin's authority in Russia), or even more troubling between multiple countries (such as disputes over the South China Sea or the 1947 Partition of India and Pakistan).

This does not mean that students in Canada, the US, Europe or the UK can be assumed to be free from surveillance and state control. The UK security apparatus, for example, has long targeted 'extremism' on campuses, and universities including individual faculty members have been required to report certain kinds of student ideas – not just plans to act, but ideas themselves – to the government. Here in Canada, we know that Muslim student organizations at U of T and elsewhere across the country have been targeted for surveillance and investigation by CSIS and RCMP officers (Nasser, 2019; Kao, 2018). It is quite possible that digital surveillance (including of U of T courses that generate a

large 'data trail' due to most activity being online) will be more heavily used in the near future in democratic countries as well as in states already known as authoritarian.

With the rise of sophisticated surveillance systems, including the use of profiling algorithms, that can trigger investigations with serious safety and human rights consequences, we can anticipate that the Chinese government will not be the only one that takes a keen interest in the online activities of our international students. Courses on anti-terrorist policing, human rights, or similar topics such as critical race and gender studies (considered "sensitive" to different governments) could be readily visible to the security agencies of countries in which U of T students taking online-only courses are physically located.

We will provide further information on the vulnerability of different kinds of students in our fuller report towards the end of the summer. But, thanks to enlightening conversations with colleagues, we can here begin to raise the alarm and call for a collegial –not administrative—discussions of the risks to students' human rights, privacy and safety that can be anticipated, and then of measures that we might collectively decide to take. ('Collegial' here including students, not just 'the professoriate'; and we distinguish collegial from administrative discussions because as already mentioned, the interests of the institution often coincide with those of its members, but at certain times interests diverge.)

That university teaching/learning is a sphere in which ideas can be examined and debated freely has long been at the core of all universities' mission. We urgently need a collective discussion about how to best ensure that human rights including freedom of expression and data protection are preserved.[5] In the absence of collectively generated policies, individual instructors alerted to

---

[5] We have initiated contact with Prof. Joseph Wong, vice-provost for international students, and also with members of the Citizen Lab, since other people or units at the university with expertise in relevant areas may already be working on the possible harms, especially to international students studying from abroad, that might occur if our own university's online learning system unwittingly exposes those students to surveillance and state control. We hope that soon we will be able to explain what various units are doing to explore and possibly remedy these issues.

the problems mentioned here might self-censor and remove all politically sensitive material from their courses – or even neglect such issues and continue with course designs that may jeopardize certain international students – both equally undesirable outcomes, especially since what is politically sensitive is not stable across time and space.

Bibliography

Amigot, M. (2019, July 10). Canvas LMS Increases Its Lead to 30 Million Users, According to Its CEO's Data. *IBL News*. https://iblnews.org/canvas-lms-increases-its-lead-to-30-million-users/

Bohaker, H., Austin, L., Clement, A., & Perrin, S. (2015). *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World*. https://tspace.library.utoronto.ca/handle/1807/73096

D2L. (2016, October 26). *D2L Selects Amazon Web Services Cloud to Improve Learning Worldwide | Press Release*. D2L. https://www.d2l.com/newsroom/releases/d2l-selects-amazon-web-services-cloud-improve-learning-worldwide/

Ghosh, S. (2019, October 18). Thoma Bravo is on a cybersecurity acquisition spree; Sophos latest to be added to cart. *CSO Online*. https://www.csoonline.com/article/3446880/thoma-bravo-is-on-a-cybersecurity-acquisition-spree-sophos-latest-to-be-added-to-cart.html

Hill, P. (2019, March 11). Instructure: Plans to expand beyond Canvas LMS into machine learning and AI. *E-Literate*. https://eliterate.us/instructure-plans-to-expand-beyond-canvas-lms-into-machine-learning-and-ai/

Instructure. (n.d.). *Security | Canvas, the Learning Management Platform*. Instructure.Com. Retrieved March 31, 2020, from https://www.instructure.com/canvas/security

Instructure. (2018a, January 11). *Acceptable Use Policy*. Instructure.Com. https://www.instructure.com/policies/acceptable-use

Instructure. (2018b, March 28). Decoding the Cloud: Answering All Your Questions (And Some More Besides). *Canvas Blog*. https://www.instructure.com/canvas/en-gb/blog/decoding-cloud-answering-all-your-questions-and-some-more-besides

Instructure. (2019, October 28). *Instructure Product Privacy Policy*. Instructure.Com. https://www.instructure.com/policies/privacy

Ivancheva, M., & Swartz, R. (2020, May 19). Universities go online during the pandemic: Who reaps the profits? *Corona Times*. https://www.coronatimes.net/universities-go-online-pandemic-profits/

Kao, J. (2018, November 12). Muslim Students' Association says executives receiving surprise visits from law enforcement. *The Varsity*. https://thevarsity.ca/2018/11/12/muslim-students-association-says-executives-receiving-surprise-visits-from-law-enforcement/

Levin, A. (2013, July 17). Outsourcing Surveillance. *PEN Canada*. https://pencanada.ca/blog/on-backdoor-information-access/

Ling, J. (2017, August 23). Canada still hasn't developed new rules for intelligence sharing with U.S. and allies. *VICE News*. https://www.vice.com/en_ca/article/a3jyn8/canada-still-hasnt-developed-new-rules-for-intelligence-sharing-with-u-s-and-allies

Marachi, R., & Quill, L. (2020). The case of Canvas: Longitudinal datafication through learning management systems. *Teaching in Higher Education*, *25*(4), 418–434. https://doi.org/10.1080/13562517.2020.1739641

Mattes, M. (2017). *The Private Side of Public Higher Education*. The Century Foundation. https://tcf.org/content/report/private-side-public-higher-education/

McCahan, S., & Hyman, A. (2017, October 19). *Update – New Learning Management Engine (PDAD&C #24) – Communications for Academic Administrators*. https://memos.provost.utoronto.ca/update-new-learning-management-engine-pdadc-24/

Mckenzie, L. (2018, July 10). Canvas catches, and maybe passes, Blackboard as top learning management system for U.S. colleges | Inside Higher Ed. *Inside Higher Ed*. https://www.insidehighered.com/digital-learning/article/2018/07/10/canvas-catches-and-maybe-passes-blackboard-top-learning

Millward, W. T. (2020, February 18). Instructure CEO to Resign and Board Approves New Private Equity Deal—EdSurge News. *EdSurge*.

https://www.edsurge.com/news/2020-02-18-instructure-ceo-resigns-and-board-approves-new-private-equity-deal

Nasser, S. (2019, August 7). When CSIS comes knocking: Amid reports of Muslim students contacted by spy agency, hotline aims to help. *CBC News*. https://www.cbc.ca/news/canada/toronto/csis-students-university-muslim-campus-1.5229670

Stalcup, K. (2020, February 5). *AWS vs Azure vs Google Cloud Market Share 2020: What the Latest Data Shows*. ParkMyCloud. www.parkmycloud.com

Strauss, V. (2020, March 20). Perspective | As schooling rapidly moves online across the country, concerns rise about student data privacy. *Washington Post*. https://www.washingtonpost.com/education/2020/03/20/schooling-rapidly-moves-online-across-country-concerns-rise-about-student-data-privacy/

Thoma Bravo. (n.d.). *Thoma Bravo | Companies*. Retrieved May 23, 2020, from https://www.thomabravo.com/companies

Thoma Bravo. (2020, March 24). Thoma Bravo Completes Acquisition of Instructure. *Cision PR Newswire*. https://www.prnewswire.com/news-releases/thoma-bravo-completes-acquisition-of-instructure-301028910.html

University of Michigan. (n.d.). *Institutional Data Resource Management Policy | Standard Practice Guides—University of Michigan*. Retrieved May 24, 2020, from https://spg.umich.edu/policy/601.12

University of Toronto. (2017, November 10). *Working Hard: Academic Toolbox Renewal*. Academic Toolbox Renewal. https://toolboxrenewal.utoronto.ca/2017/11/10/working-hard/

Wan, T. (2019, July 10). Instructure's Age of Adolescence: A Conversation With CEO Dan Goldsmith - EdSurge News. *EdSurge*. https://www.edsurge.com/news/2019-07-10-instructure-s-age-of-adolescence-a-conversation-with-ceo-dan-goldsmith

WikiLeaks. (2018, October 11). *WikiLeaks—Map of Amazon's Data Centers*. https://wikileaks.org/amazon-atlas/map/

Research Group